(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 685 111**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **91 15458**

(51) Int Cl⁵ : G 06 K 9/62, G 06 F 13/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 12.12.91.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : 18.06.93 Bulletin 93/24.

(56) Liste des documents cités dans le rapport de recherche : *Se reporter à la fin du présent fascicule.*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *SCHLUMBERGER INDUSTRIES Société Anonyme* — FR.

(72) Inventeur(s) : Guion Christian.

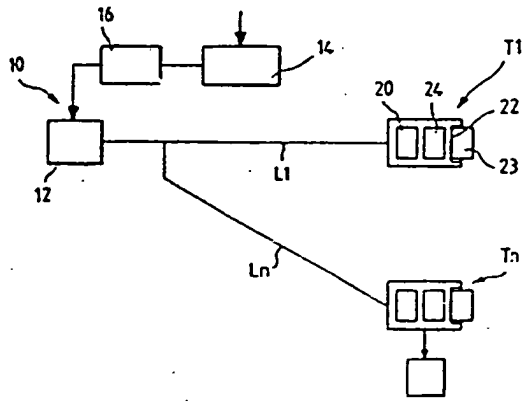
(73) Titulaire(s) :

(74) Mandataire : Cabinet Beau de Loménie.

(54) Installation de vérification de l'information d'identification de titres au regard d'une liste de titres frappés d'opposition.

(57) L'invention concerne une installation pour comparer le numéros d'identification de titres (cartes de paiement, chèque, etc.) à une liste de numéros frappés d'opposition.

Une station centrale (10) émet en permanence cycliquement des informations représentatives des numéros frappés d'opposition vers chaque terminal (T1 à Tn) de vérification des titres (23). Chaque terminal comporte des circuits (24) pour comparer "au vol" les informations reçues et le numéro du titre à vérifier.



FR 2 685 111 - A1

Installation de vérification de l'information d'identification de titres au regard d'une liste de titres frappés d'opposition.

La présente invention a pour objet une installation de vérification de l'information d'identification de titres au regard d'une liste d'informations d'identification de titres frappés d'opposition présentant un attribut particulier.

Il existe maintenant un grand nombre de titres permettant soit d'obtenir de l'argent soit de régler un certain nombre de dépenses soit encore d'obtenir certaines prestations. Parmi ces titres, on peut citer les chèques bancaires et analogues, les cartes bancaires à pistes magnétiques et les cartes bancaires ou cartes de crédit ou encore carte de paiement à circuits électroniques.

Les progrès effectués dans les technologies utilisées pour la fabrication de ces titres permettent une assez bonne protection contre la contrefaçon physique de ces titres ou la mise en service de titres apocryphes.

On peut citer des techniques sécurisées d'impression des chèques, l'utilisation de pistes magnétiques à haute densité d'enregistrement dans le cas des cartes à mémoire magnétique, et pour les cartes électroniques, la protection réalisée par le caractère intégré de la mémoire et des circuits de la carte ainsi que les techniques liées au lecteur de cartes protégeant contre des cartes falsifiées.

Cependant, ces progrès ne protègent pas totalement contre l'utilisation indue de ces titres.

Cela se présente en particulier dans le cas où ces titres sont dérobés à leur légitime propriétaire et utilisés frauduleusement. C'est également le cas si l'organisme émetteur (par exemple une banque) désire priver le détenteur légitime du titre (carte bancaire) du droit de l'utiliser. C'est encore le cas si l'organisme émetteur (par exemple une banque) sans interdire l'usage du titre veut attirer l'attention du prestataire de service (par exemple le commerçant) sur ce titre. On sait que ces différents titres comportent chacun une information

d'identification stockée sur le titre de façon lisible dans le cas des chèques ou sous une forme codée dans le cas des cartes magnétiques ou électroniques. Cette information d'identification est appelée le plus souvent "code porteur" ou "code confidentiel".

Pour se prémunir contre les conséquences de cette utilisation abusive, le titulaire légitime du titre fait une déclaration pour faire opposition à l'utilisation ultérieure du titre en question. A partir de ces déclarations, l'organisme qui gère l'utilisation des titres établit des listes de titres frappés d'opposition ou listes noires. La liste noire est donc la liste complète de tous les numéros de cartes ou de chèques frappés d'opposition. La sécurité totale d'utilisation des titres impose donc qu'avant ou durant l'utilisation de chacun de ces titres, on vérifie que le numéro d'identification du titre ne figure pas sur la liste d'opposition. Avec la décentralisation des lieux d'utilisation des différents titres, cette vérification du code porteur au regard des listes d'opposition devient de plus en plus difficile.

Dans beaucoup de points de vente, il n'existe pas de moyen simple et/ou économique pour vérifier que les cartes bancaires sont en opposition. Soit les points de vente sont équipés de "facturettes" manuelles ou automatiques avec une vérification du numéro d'identification par appel téléphonique ; soit on trouve des terminaux "off line" dans lesquels, on dispose d'une liste noire réduite à quelques milliers de numéros. Dans ce cas, la vérification complémentaire peut se faire par appel téléphonique automatique depuis le terminal vers une station centrale comportant l'intégralité de la liste d'opposition. Dans le cas des magasins équipés de terminaux "on line" ou avec appel systématique à la station centrale de contrôle, on peut effectuer la vérification de la présence en liste d'opposition au prix d'une communication par transaction, ce qui est long et onéreux.

Pour remédier à cet inconvénient, on a proposé une solution qui permet de réduire très sensiblement la nécessité d'appels téléphoniques vers la station centrale. Ce procédé dit

"liste grise" consiste à renuméroter les cartes (informations d'identification à 19 chiffres) par un algorithme decodage et de compactage de façon à produire, par exemple, pour chaque information d'identification un numéro plus court à 6, 8 ou 10 chiffres.

On comprend qu'ainsi chaque numéro court est associé à un certain nombre de numéros d'identification de cartes. Dans ce système, si au moins un numéro d'identification complet est frappé d'opposition, le numéro court associé sera considéré également comme frappé d'opposition ou plus précisément douteux. L'ensemble des numéros courts douteux sont mémorisés au niveau de chaque terminal. Lorsqu'une carte est présentée au terminal, celui-ci compare sur le site l'information d'identification de la carte ou plus précisément le numéro court associé à ce numéro à la liste des numéros courts douteux. Si le numéro court n'y figure pas, la carte est sûrement bonne. Si le numéro court y figure, il y a un doute et ce doute doit être levé en appelant la station centrale détenant la totalité de la liste des numéros frappés effectivement d'opposition. On comprend que cette nécessité, dans certains cas, de vérification supplémentaire alourdit très sensiblement le système. En outre, on comprend qu'il n'est pas possible à distance de réactualiser en permanence dans chaque terminal la liste des numéros courts douteux. Il s'écoule nécessairement un certain laps de temps entre la déclaration de perte ou de vol, faite auprès de l'organisme gestionnaire et la prise en compte de cette déclaration dans les listes de numéros longs frappés d'opposition et donc dans la liste des numéros douteux stockés dans les différents terminaux.

Un objet de la présente invention est de fournir une installation de vérification de l'information d'identification de titres qui présente un taux très élevé de sécurité sans nécessiter d'appel téléphonique supplémentaire et qui permette également d'effectuer cette vérification par comparaison à une liste d'opposition mise à jour avec une périodicité très courte.

Pour atteindre ce but, selon l'invention, l'installation de vérification de l'information d'identification de titres au regard d'une liste d'informations d'identification de titres frappés d'opposition comprend une station centrale dans laquelle ladite liste est mémorisée, une pluralité de terminaux dans lesquels lesdits titres peuvent être introduits en vue de la vérification de leur information d'identification et des moyens de transmission d'informations sous forme numérique entre ladite station centrale et lesdits terminaux, l'installation se caractérisant en ce que :

- ladite station centrale comprend des moyens pour émettre cycliquement vers chaque terminal des informations en relation avec ladite liste d'informations d'identification de titres frappés d'opposition, et en ce que chaque terminal comprend des moyens pour mémoriser l'information d'identification du titre à vérifier, des moyens pour traiter les informations reçues à chaque cycle de transmission, des moyens pour comparer en permanence ladite information mémorisée à l'ensemble des informations traitées reçues cycliquement pendant au moins un cycle, et des moyens pour déterminer, en fonction des résultats de ladite comparaison avec une probabilité au moins égale à ladite valeur prédéterminée si ladite information d'identification mémorisée appartient à ladite liste d'informations d'identification de titres frappés d'opposition .

On comprend qu'ainsi chaque terminal n'a pas besoin de disposer d'une mémoire de masse importante puisque la comparaison entre les différentes informations reçues et l'information d'identification de la carte ou du titre à vérifier se fait au vol. En outre, comme l'ensemble des informations correspondant à l'ensemble de la liste des numéros frappés d'opposition se fait cycliquement à partir d'une station centrale, il est possible de réactualiser pratiquement en temps réel ladite liste lors de sa transmission cyclique. Le cycle peut avoir u ne durée très longue, "infinie", dans certains cas d'application comme on l'expliquera ultérieurement.

Selon des modes de mise en oeuvre préférés qui seront explicités ultérieurement, les informations transmises correspondant aux informations d'identification frappées d'opposition résultent de l'application d'algorithmes de codage et de compactage à la liste complète des informations d'identification possible des titres. On réduit ainsi très sensiblement la durée de chaque cycle de transmission des informations et donc la durée de l'opération de vérification au niveau du terminal, du fait que le nombre total d'informations à transmettre est très sensiblement réduit.

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description qui suit de plusieurs modes de mises en oeuvre de l'invention donnés à titre d'exemples non limitatifs.

La description se réfère aux figures annexées sur lesquelles :

- la figure 1 est un diagramme simplifié de l'ensemble de l'installation de vérification ; et,

- la figure 2 est un schéma des circuits d'un terminal de l'installation.

Avant de décrire plus en détails l'invention, il est important de rappeler certains éléments concernant l'établissement des listes d'opposition ou des listes noires dans différents pays.

En France, la liste noire des cartes bancaires contient environ 1,5 million de numéros de cartes. Un numéro de carte bancaire peut avoir 19 chiffres. La liste noire des grands pays tels que les Etats-Unis d'Amérique peut atteindre de 10 à 20 millions de numéros. La plupart des pays européens émettent des listes noires comprises entre 100 000 et 2 millions de numéros.

Comme on l'a déjà indiqué succinctement, le principe de l'installation consiste à relier la station centrale détenant la liste noire complète des numéros frappés d'opposition à chacun des terminaux de gestion des titres par des moyens de transmission d'informations sous forme numérique. Chaque terminal est dépourvu de mémoire de masse. Chaque terminal comporte comme on

l'expliquera ultérieurement des circuits de traitement permettant de décoder au vol les informations successives transmises dans chaque cycle de transmission d'informations. Par ailleurs, le terminal est capable de lire et de mémoriser temporairement l'information d'identification du titre à vérifier. La comparaison entre le numéro d'identification à vérifier et les différentes informations transmises et traitées se fait donc au vol. Si le numéro d'identification de la carte n'a pas été trouvé parmi les informations transmises, cette carte sera jugée comme bonne avec une probabilité dépendant de la nature des informations effectivement transmises et prises en compte pour la comparaison comme on l'explicitera ultérieurement.

En se référant tout d'abord à la figure 1, on va décrire l'ensemble de l'installation. Celle-ci comprend une station centrale 10 constituée par un émetteur 12, une installation informatique de stockage de liste noire 14, et des moyens de traitement 16. L'installation 14 comporte la liste d'opposition complète avec les informations d'identification de titres (ultérieurement appelée numéros de titres) classés par ordre croissant. On comprend qu'on peut ainsi introduire dans cette liste en temps réel les nouveaux numéros frappés d'opposition ou, au contraire, retirer ceux qui ne le sont plus au fur et à mesure des déclarations faites par les titulaires de titres. Le circuit de traitement informatique 16 a pour objet d'appliquer à la liste complète des numéros frappés d'opposition un ou plusieurs algorithmes de codage et de compactage afin d'obtenir l'ensemble des informations qui sont effectivement émises par l'émetteur 12 de façon cyclique. L'émetteur 12 est relié aux différents terminaux de traitement des titres référencés T1,T2,TN par des liaisons de transmission d'informations sous forme numérique référencées L1 etc... LN. Chaque terminal T comprend une portion de traitement des informations reçues référencée 20, une section 22 pour recevoir le titre à vérifier 23 et en extraire son numéro d'identification et une section 24 de comparaison entre le numéro d'identification du titre vérifié et les informations reçues

cycliquement par le ...rcuit 20.

De préférence, les liaisons de transmission en informations sous forme numérique Li sont des canaux de télévision qui présentent un débit de 6 M bits par seconde. Si l'on prend le cas d'une liste noire comportant 1.500.000 numéros, qu'on admet une efficacité de compactage de deux, ce qui correspond à 32 bits par numéro de la liste noire, on est donc amené à diffuser la liste de manière répétitive et cyclique, soit environ 50 M bits en 10 secondes. L'émetteur 12 module par exemple un des signaux vidéo de manière numérique pour transmettre effectivement ces informations. L'unité de traitement 20 de chaque terminal décode au fur et à mesure de leur réception les informations et les compare dans le circuit 24 à l'information d'identification du titre à vérifier. A chaque instant, le numéro à vérifier est soit inférieur soit égal soit supérieur à ce numéro. Si le comparateur passe de la situation supérieure à la situation inférieure sans rencontrer le signe égal l'appareil considère que le numéro est valide. Si une information transmise est brouillée la relation d'ordre va être perturbée, ce qui sera détecté. Dans ce cas, on utilisera un deuxième cycle de transmission d'informations pour effectuer la vérification.

Une solution pour diminuer le nombre d'informations numériques de base (nombre de bits) à transmettre consiste non pas à transmettre directement la suite des numéros frappés d'opposition mais à transmettre au début de chaque cycle le numéro frappé d'opposition le plus faible et à transmettre la différence entre ce premier numéro et le numéro immédiatement suivant également frappé d'opposition. On comprend que la différence s'exprime par un nombre inférieur à la valeur du numéro à transmettre ce qui réduit donc le nombre de bits nécessaires à la transmission de cette information.

Pour réduire encore le temps de transmission de l'ensemble des informations associées aux numéros frappés d'opposition vers chacun des terminaux, on peut utiliser la mise en oeuvre d'un algorithme de codage et de compactage qui permet de

passer des numéros possibles complets à 19 chiffres des titres à un numéro court par exemple à 8 chiffres. On comprend qu'ainsi à chaque numéro complet de titre il correspond un seul numéro court parmi les 10^8 numéros courts et que à un numéro court il correspond un certain nombre de numéros complets dépendant de la fonction de compactage mise en oeuvre. Ces fonctions peuvent être de nature très différente. De préférence, elles associent des numéros complets à des numéros courts de façon aléatoire de telle manière que l'on ait une probabilité sensiblement égale pour qu'un numéro court soit "douteux". Si un parmi l'ensemble des numéros complets associés à un numéro court est frappé d'opposition le numéro court sera lui-même considéré comme douteux. Dans ce mode de réalisation, chaque terminal reçoit cycliquement des informations fournissant la liste des numéros courts douteux.

D'un point de vue concret la transmission de ces informations consiste dans la transmission en série d'une suite de valeurs binaires 1 et 0, le "1" correspondant par exemple à un numéro "douteux" et le "0" à un numéro valide. Si l'algorithme de compactage associe aux numéros complets 10^8 numéros courts, l'information transmise pour cet algorithme consiste en une suite de 10^8 valeurs binaires. L'informatioon transmise comporte donc 10^8 bits. Le rang de chaque information binaire représente l'état du numéro court égal à ce rang. Cette valeur binaire est égale à 1 si le numéro court est "douteux" et elle est égale à 0 si le numéro court est "valide".

Par mise en oeuvre de l'algorithme correspondant le numéro de la carte à vérifier est remplacé par le numéro court associé et on effectue la comparaison correspondante. Si l'information binaire dont le rang est égal au numéro court de la carte à vérifier est à l'état "0", la carte est sûrement valide car aucun numéro complet de carte associé à ce numéro court n'est frappé d'opposition. Au contraire si son état binaire est "1", il y a doute. Si l'on considère le cas particulier où le nombre de numéros de cartes frappés d'opposition est égal à 1.500.000 si l'algorithme de codage et de compactage fait passer de numéros à

19 chiffres à des numéros courts à 8 chiffres on a donc 1,5 % de cas douteux. On a donc 1,5 % de cas douteux, c'est-à-dire de cas dans lesquels on ne peut dire si la carte ou le titre est bon ou frappé d'opposition. Le temps de transmission d'un cycle complet correspond toujours à 50 M bits soit 10 secondes.

Pour résoudre l'incertitude liée aux cas douteux, l'invention propose de mettre en oeuvre plusieurs lois de compactage et de codage non correlées entre-elles, chaque loi permettant de passer de l'ensemble des numéros longs ou complets à un même nombre de numéros courts par exemple 10^8.

Chaque numéro court qui correspond à au moins un numéro long frappé d'opposition est "douteux" (valeur binaire 1) et chaque numéro court associé à des numéros longs dont aucun n'est frappé d'opposition est "valable" (valeur binaire 0). Si l'on appelle a le pourcentage statistique de numéros courts douteux parmi l'ensemble des numéros courts, la probabilité pour qu'un numéro de titre soit considéré comme douteux lors de l'opération de comparaison est de a/100. On définit un deuxième algorithme de codage et de compactage A2 non correlé au premier et dans lequel le pourcentage statistique de numéros courts douteux est aussi égal à a. Si l'on compare successivement le numéro à vérifier à la liste de numéros courts douteux obtenus à partir du premier algorithme A1 puis à la liste des numéros courts douteux obtenus à partir du deuxième algorithme A2, on obtient les résultats suivants. Si le numéro à vérifier n'appartient à aucune des listes de numéros courts douteux ou seulement à une des deux listes le numéro est valide. C'est seulement dans le cas où le numéro à vérifier appartient simultanément aux deux listes que son état reste douteux. La probabilité pour que cette situation se présente est donc égale à $a^2\ 10^{-4}$.

Plus généralement, on comprend que si l'on définit N algorithmes de compactage non corrélés présentant chacun un pourcentage a de cas douteux, l'exploitation des N comparaisons entre le numéro à vérifier et les N listes permet de ne laisser subsister qu'une probabilité de cas douteux égale à $a^N\ 10^{-2N}$.

On comprend qu'en choisissant N suffisamment grand, on peut rendre cette probabilité très faible. Cela signifie que, dans de telles conditions, on pourra assimiler le fait que le numéro à vérifier appartienne à toutes les listes de numéros douteux du fait que le numéro à vérifier est frappé d'opposition avec un risque d'erreur très faible.

On comprend également qu'il est important de faire un compromis entre la valeur de a et la valeur de N pour réduire le plus possible le nombre de bits à transmettre dans chaque cycle tout en maintenant une probabilité d'erreur très réduite.

On comprend que dans un cycle de transmission d'informations, on trouvera un nombre de sous cycles égal au nombre N d'algorithmes de compactage et de codage utilisés. Chaque sous cycle comportera donc des informations représentatives de la liste des numéros courts possibles douteux ou valides résultant de la mise en oeuvre de chacun des algorithmes. A la réception, c'est-à-dire au niveau de chaque terminal, on comparera le numéro court associé au titre à vérifier avec les numéros courts correspondant à chacun des sous cycles. Si le numéro court à vérifier ne figure pas dans au moins une des listes, le titre est valide. Au contraire, si le numéro à vérifier appartient à chacune des listes transmises dans les sous cycles le titre demeure douteux et il sera considéré finalement comme non valide.

D'un point de vue concret, chaque sous-cycle est constitué par une suite de, par exemple, 10^8 bits dont les rangs correspondent aux numéros courts possible. Chaque bit est, à la valeur binaire 1 ou 0 selon que le numéro court correspondant est douteux ou valide. Le terminal lit le numéro complet du titre à vérifier et détermine par mise en oeuvre des N algorithmes de compactage non corrélés les N numéros courts correspondants. Pour chaque sous-cycle, les circuits du terminal lisent l'état binaire du bit dont le rang est égal au numéro court du titre obtenu par mise en oeuvre de l'algorithme de compactage associé à ce sous-cycle. A la suite de ces N lectures, si les N états binaires lus sont tous égaux à 1 (douteux), le titre est déclaré non valide.

Au contraire, si au moins un des N états binaires lus est égal à 0 (valide), le titre est déclaré valide.

Si dans la suite des bits transmis, un pourcentage très élevé de ces bits a un même état binaire (1 ou 0), par exemple s'il y a 99% de bits à zéro, il sera plus économique de transmettre comme informations dans chaque sous-cycle la longueur des intervalles codés entre deux bits consécutifs à zéro.

Dans la description précédente, on a considéré que l'ensemble des informations étaient transmises par l'intermédiaire d'un seul canal de transmission numérique. Dans le cas de câbles de télévision en particulier ou dans le cas où la station centrale et les terminaux sont installés en un réseau autonome, on peut disposer de plusieurs canaux au moins partiellement libres. Pour réduire la durée du cycle de transmission des informations, on peut donc fractionner l'ensemble des numéros complets des titres en plusieurs groupes la fonction de compactage étant appliquée à chaque groupe pour obtenir autant de groupes denuméros courts possibles et transmettre un groupe de numéros courts par chacun des canaux. Il est bien sûr nécessaire dans ce cas que le terminal puisse détecter sur quel canal il doit rechercher l'information de vérification. Ce problème peut être résolu définissant un algorithme qui permet d'indiquer pour chaque information d'identification d'un titre le canal à prendre en cours.

En outre, il est possible que le terminal soit capable d'effectuer la vérification pour des titres de types différents, par exemple des chèques, des cartes magnétiques ou des cartes à mémoire électronique. Dans ce cas, il est possible de spécialiser les canaux de transmission pour l'émission des informations relatives à chaque type de titre.

Il va également de soi que, comme on l'a expliqué la comparaison se fait au vol entre le numéro du titre à vérifier et l'ensemble des informations reçues par le terminal, il est possible de procéder à la vérification simultanée de plusieurs titres, l'information d'identification de chaque titre étant stockée temporairement en mémoire.

En se référant maintenant à la figure 2, on va décrire plus en détail la partie du terminal de vérification associée aux opérations de vérification de l'information d'identification. Cette partie 20,24 comprend tout d'abord un sélecteur de signaux haute fréquence 40 qui reçoit les informations transmises par la ligne L1, cette ligne pouvant comporter plusieurs canaux parallèles. Les informations reçues par le sélecteur 40 sont transmises à un circuit modulateur 42 qui élabore les informations numériques sous forme binaire contenues dans l'émission. L'ensemble des circuits de traitement du terminal est géré par un microprocesseur 44 qui commande par sa sortie a la sélection des canaux dans le cas où la ligne en comporte plusieurs. Le microprocesseur reçoit sur son entrée b au vol les informations numériques extraites par le modem 42. Ces informations sont également appliquées à l'entrée d'un circuit comparateur 46. Le terminal ou plus précisément l'ensemble des circuits 20,24 est relié à un lecteur de cartes à mémoire électronique 50 à un lecteur de cartes magnétiques 52 et à un lecteur de chèques 54. Chacun de ces lecteurs est capable de mémoriser temporairement l'information d'identification du titre correspondant. Cette information est transmise au microprocesseur 44 qui convertit cette information par la mise en oeuvre du ou des algorithmes de compactage et de codage qui ont été utilisés lors de l'émission des informations transmises par la station centrale 10. Cette information codée est également appliquée à l'entrée du comparateur 46. Comme on l'a indiqué antérieurement si le numéro du titre à vérifier n'apparaît pas dans la liste des informations transmises ou n'apparaît que dans certaines des listes transmises au cours d'un même cycle dans le cas de l'utilisation de plusieurs algorithmes de codage et de compactage, le titre est considéré comme valide et le microprocesseur 44 transmet une instruction d'autorisation de prestation vers le terminal point de vente 56. Si au contraire, ce numéro apparaît sur la liste ou sur toutes les listes, l'opération est interdite.

Comme on l'a indiqué précédemment, le terminal ou plus précisément les circuits 20,24 doivent disposer des algorithmes de

compactage et de codage utilisés dans la station centrale.

Plusieurs solutions sont possibles pour mettre ces logiciels à la disposition du terminal. Le logiciel peut être transmis cycliquement au terminal par un des canaux des lignes de transmission. Une autre solution consiste à stocker dans une mémoire permanente l'ensemble de ces logiciels. Pour sécuriser ce stockage d'informations, il est possible de stocker ce logiciel dans un microprocesseur monochip intégré dans une carte à mémoire électronique par exemple 58. Cette carte 58 est amovible par rapport à un lecteur de cartes spécialisé 60 qui est relié au microprocesseur 44. Une solution intermédiaire consiste à stocker dans le microprocesseur de la carte 58 l'ensemble des logiciels associés aux algorithmes de codage et de compactage à l'exception de certains paramètres. Ces paramètres sont transmis périodiquement par la ligne de transmission L en faisant varier périodiquement la valeur de ces paramètres. Cette variation est évidemment faite en synchronisme avec les variations correspondantes au niveau du circuit de traitement 16 de la station centrale 10. Avec ce mode de réalisation, on voit qu'on dispose d'algorithmes de codage dynamiques qui rendent une fraude au niveau du terminal particulièrement difficile.

Dans le cas de mise en oeuvre de l'installation qui utilise plusieurs algorithmes non corrélés de compactage, on comprend que la notion de cycle de transmission n'est plus significative. En effet, ce qui importe est que N algorithmes de compactages correspondant à la probabilité requise, soient exploités pour vérifier la validité du titre. En d'autres termes, la vérification d'un titre peut chevaucher de cycles successifs à condition que N sous-cycles consécutifs soient pris en compte.

Il est également possible de prévoir que chaque "cycle" comporte N sous cycles associés à N algorithmes non corrélés, et que la comparaison a seulement N' tables consécutives de N' sous cycles consécutifs soit suffisante pour obtenir la probabilité souhaitée. Dans ce cas, les circuits de traitement du terminal comportent un compteur de nombres de sous cycles et l'opération de

vérification est achevée lorsque le compteur atteint la valeur N'.

Enfin, chaque terminal peut comprendre des moyens pour facturer les opérations de vérifications des titres à l'aide du terminal. Dans ce but, chaque terminal peut comporter un compteur qui est incrémenté lors de chaque opération de vérification, par exemple à l'émission de chaque information de validité ou de non validité du titre à vérifier. Il est également possible de précharger le compteur à une valeur prédéterminée correspondant à un pré paiement effectué par le détenteur du terminal de vérification, le compteur étant décrémenté d'une unité après chaque vérification.

REVENDICATIONS

1. Installation de vérification de l'information d'identification de titres au regard d'une liste d'informations d'identifications de titres (23) frappés d'opposition, comprenant une station centrale (10) dans laquelle ladite liste est mémorisée (14), une pluralité de terminaux (T1 à Tn) dans lesquels lesdits titres peuvent être introduits en vue de la vérification de leur information d'identification, et des moyens de transmission d'informations sous forme numérique entre ladite station centrale et lesdits terminaux, caractérisée en ce que ladite station centrale (10) comprend des moyens (12) pour émettre cycliquement et simultanément vers chaque terminal (T1 à Tn) des informations en relation avec ladite liste d'informations d'identification de titres frappés d'opposition, et en ce que chaque terminal comprend des moyens (22, 50) pour mémoriser l'information d'identification du titre à vérifier, des moyens (24) pour traiter les informations reçues à chaque cycle de transmission, des moyens pour comparer (46) en permanence ladite information mémorisée à l'ensemble des informations traitées reçues cycliquement durant au moins un cycle, et des moyens pour déterminer, en fonction des résultats de ladite comparaison, avec une probabilité au moins égale à une valeur prédéterminée, si ladite information d'identification mémorisée appartient à ladite liste d'informations d'identification de titres frappés d'opposition.

2. Installation selon la revendication 1, caractérisée en ce que lesdits moyens de transmission (L1, Ln) sont choisis parmi les réseaux câblés de télévision, les réseaux hertziens et les réseaux radio.

3. Installation selon l'une quelconque des revendications 1 et 2, caractérisée en ce que lesdites informations d'identification sont des informations numériques, en ce que lesdites informations transmises dans un même cycle comprennent l'information d'identification frappée d'opposition ayant la valeur la plus faible et des informations représentant chacune la

différence entre une information d'identification frappée d'opposition et l'information d'identification frappée d'opposition ayant la valeur immédiatement suivante et en ce que lesdits moyens de traitement de chaque terminal sont aptes à restituer à partir des informations reçues la liste complète desdites informations d'identification frappée d'opposition.

4. Installation selon l'une quelconque des revendications 1 à 3, caractérisée en ce que ladite station centrale (10) comprend des moyens (16) pour associer à chaque information d'identification frappée d'opposition une information codée unique exprimée avec un nombre d'informations élémentaires inférieur à celui des informations élémentaires servant à écrire ladite information d'identification frappée d'opposition par mise en oeuvre d'un algorithme de compactage, en ce que lesdites informations émises cycliquement vers lesdits terminaux comprennent lesdites informations codées et en ce que chaque terminal comprend des moyens pour appliquer à ladite information d'identification à vérifier ledite algorithme de compactage, et en ce que lesdits moyens de comparaison (46) comparent lesdites informations codées reçues durant au moins un cycle à ladite information d'identification codée à vérifier.

5. Installation selon l'une quelconque des revendications 1 à 3, caractérisée en ce que ladite station centrale (10) comprend des moyens (16) pour mettre en oeuvre N algorithmes de compactage non corrélés, chaque algorithme de compactage associant à une information d'identification frappée d'opposition une information codée unique exprimée avec un nombre d'informations élémentaires inférieur à celui des informations élémentaires servant à écrire une information d'identification frappée d'opposition, en ce que lesdites informations émises dans chaque cycle vers lesdits terminaux comprennent N sous-cycles successifs d'informations, chaque sous-cycle comprenant lesdites informations codées par la mise en oeuvre de chacun desdits algorithmes de compactage, et en ce que chaque terminal (T1, Tn) comprend des moyens (44) pour appliquer à ladite information

d'identification à vérifier lesdits N algorithmes de compactage, en ce que lesdits moyens de comparaison (46) comparent lesdites informations codées dans un même sous-cycle à ladite information à vérifier codée avec l'algorithme de compactage correspondant, et en ce que les moyens de détermination délivre un signal de vérification en réponse à N' comparaisons effectuées avec les informations codées reçues dans N' sous-cycles consécutifs des N sous-cycles, avec N'< N.

6. Installation selon la revendication 5, caractérisée en ce que ledit titre à vérifier est déclaré invalide si les N' comparaisons montrent que ladite information à vérifier codée figure dans les informations de chacun des N' sous-cycles d'informations.

7. Installation selon l'une quelconque des revendications 5 et 6, caractérisée en ce que le nombre N' de comparaisons effectivement mises en oeuvre est déterminé en fonction de ladite probabilité prédéterminée.

8. Installation selon l'une quelconque des revendications 5 à 8, caractérisée en ce que lesdites informations transmises dans un même sous-cycle comprennent l'information d'identification codée ayant la valeur la plus faible et des informations représentant chacune la différence entre une information d'identification codée et l'information d'identifivation codée ayant la valeur immédiatement supérieure et en ce que lesdits moyens de traitement de chaque terminal sont aptes à restituer, à partir des informations reçues la liste complète desdites informations d'identification codées.

9. Installation selon la revendication 5, caractérisée en ce que les informations transmises dans chaque sous-cycle consistent en une succession de valeurs binaires transmises en série, chaque bit ayant un rang correspondant à la valeur codée obtenue par mise en oeuvre de l'algorithme de ocmpactage associé audit sous-cycle à l'ensemble des informations d'identification des titres, et qui a une première valeur binaire (1) si au moins une information d'identification correspondant à cette information

codée est frappée d'opposition, et une deuxième valeur binaire (0) dans le cas contraire ; et en ce que ladite comparaison consiste à détecter la valeur binaire de l'information codée transmise ayant un rang égal à l'information codée obtenue par mise en oeuvre de l'algorithme de compactage correspondant à l'information d'identification du titre à vérifier, ledit titre à vérifier étant déclaré non valide seulement si les N' valeurs binaires détectées dans les N' sous-cycles consécutifs sont toutes égales à ladite première valeur binaire (1).

10. Installation selon l'une quelconque des revendications 4 à 9, caractérisée en ce que chaque terminal comprend un microprocesseur monochip apte à recevoir et/ou mémoriser les informations nécessaires à la mise en oeuvre du ou des algorithmes de compactage.

11. Installation selon la revendication 10, caractérisée en ce que ledit microprocesseur monochip est préprogrammé avec l'ensemble des informations nécessaires à la mise en oeuvre du ou desdits algorithmes à l'exception de certains paramètres, et en ce que les valeurs desdits paramètres sont transmises périodiquement audit microprocesseur par lesdits moyens de transmission à partir de ladite station centrale.

12. Installation selon l'une quelconque des revendications 10 et 11, caractérisée en ce que ledit microprocesseur monochip est monté sur un support amovible (58) et en ce que ledit terminal (Ti) comprend des moyens (60) pour relier électriquement ledit microprocesseur au reste des circuits dudit terminal.

13. Installation selon l'une quelconque des revendications 1 à 12, caractérisée en ce que lesdits moyens de transmission (L1 à Ln) d'informations sous forme numérique entre ladite station centrale (10) et chaque terminal (T1 à Tn) comprennent n canaux parallèles de transmission, et ce ce que l'ensemble des informations à transmettre est partagé en k groupes, chaque groupe d'informations étant transmis par un desdits canaux.

14. Installation selon la revendication 13, caractérisée en ce que chaque terminal (T1 à Tn) comprend des moyens (40, 44) pour déterminer à partir de l'information d'identification du titre à vérifier celui des n canaux sur lequel sont transmises les informations relatives à celui des k groupes auxquels appartient ladite information d'identification à vérifier.

15. Installation selon la revendication 14, caractérisée en ce que les titres à vérifier appartiennent à k types de titres distincts et en ce que le nombre de n canaux de transmission est égal au nombre k de types de titres.

16. Installation selon l'une quelconque des revendication 1 à 15, caractérisée en ce que chaque terminal comporte en outre des moyens de décompte du nombre de vérifications effectuées en vue de la facturation desdites vérifications.

17. Installation selon l'une quelconque des revendications 1 à 15, caractérisée en ce que chaque terminal comporte en outre des moyens de comptage du nombre de vérifications effectuées et des moyens pour interrompre la liaison entre ladite station centrale et ledit terminal lorsque le nombre de vérifications atteint une valeur prédéterminée.

18. Installation selon l'une quelconque des revendications 1 à 17, caractérisée en ce que chaque terminal (T1 à Tn) comprend un sélecteur de canal haute fréquence (40) et des moyens de décodage numérique pour recueillir les informations numériques transmises par lesdits moyens de transmission des moyens de comparaison pour comparer succesivement lesdites informations reçues et l'information d'identification lue dans le titre à vérifier (23) et au moins au moyen de traitement du titre à vérifier.

19. Installation selon la revendication 18, caractérisée en ce que lesdits moyens de traitement de titres comprennent au moins un des moyens suivants : lecteur de cartes à mémoire électronique (50), lecteur de cartes à piste magnétique (52), lecteur de chèques bancaires (54).

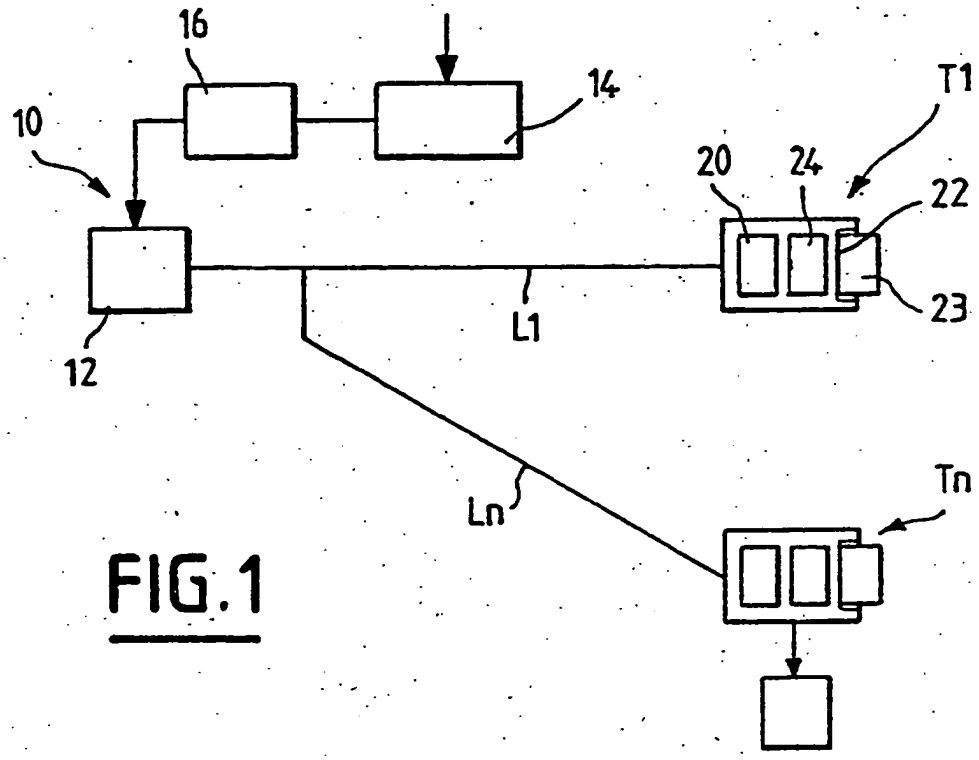

16
14
10
T1
20
24
22
23
L1
12
Ln
Tn

FIG.1

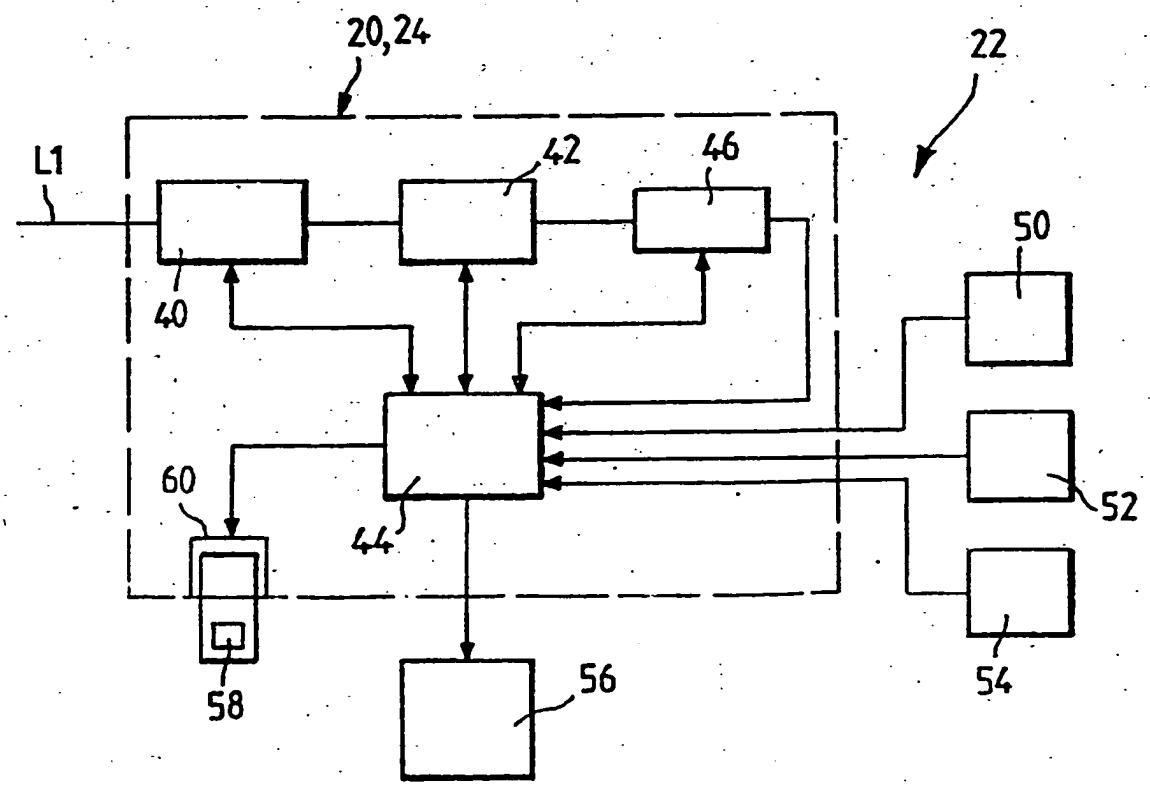

20,24
22
L1
42
46
50
40
60
44
52
58
56
54

FIG.2

2685111

N° d'enregistrement national

FR 9115458
FA 467812

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL de la PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	US-A-3 798 602 (J.F. HYNES) * abrégé; figures 1,2 * * colonne 2, ligne 30 - ligne 57 * * colonne 3, ligne 10 - colonne 5, ligne 19 *	1,2,18, 19
A	---	10-12
A	EP-A-0 274 191 (VISA INTERNATIONAL SERVICE ASSOCIATION) * abrégé; figures * * page 3, ligne 50 - page 4, ligne 50 * * page 5, ligne 7 - page 7, ligne 25 * * page 8, ligne 16 - page 9, ligne 23 *	1,2,4-7, 9-12,18, 19
A	---	
A	US-A-3 612 660 (W.S. MILLER) * abrégé; figures 2,3 * * colonne 1, ligne 1 - ligne 75 *	1,3,8
A	---	
A	EP-A-0 254 595 (TRINTECH)	
A	---	
A	GB-A-2 092 345 (J.W. HALPERN)	
A	---	
A	EP-A-0 349 413 (SCHLUMBERGER INDUSTRIES)	

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G07F
G06F

Date d'achèvement de la recherche: 09 SEPTEMBRE 1992

Examinateur: DAVID J.Y.H.

1

EPO FORM 1503 03.82 (P0413)

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant